Calhoun: The NPS Institutional Archive

DSpace Repository

Theses and Dissertations | 1. Thesis and Dissertation Collection, all items

2006-06

Development of methodical social engineering taxonomy project

Laribee, Lena

Monterey, California. Naval Postgraduate School

http://hdl.handle.net/10945/2734

This publication is a work of the U.S. Government as definedin Title 17, United States Code, Section 101. As such, it is in thepublic domain, and under the provisions of Title 17, United StatesCode, Section 105, is not copyrighted in the U.S.

Downloaded from NPS Archive: Calhoun

http://www.nps.edu/library

Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

DEVELOPMENT OF METHODICAL SOCIAL ENGINEERING TAXONOMY PROJECT

by

Lena Laribee

June 2006

Thesis Co-Advisors: Craig H. Martell
Neil C. Rowe

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** June 2006	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: **Development of Methodical Social Engineering Taxonomy Project**			**5. FUNDING NUMBERS**
6. AUTHOR(S) Lena Laribee			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) OSD - Directorate of Operational Testing and Evaluation ATTN: Mr. Stephen Gates 1700 Defense Washington, DC 20301			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

Since security is based on trust in authenticity as well as trust in protection, the weakest link in the security chain is often between the keyboard and chair. We have a natural human willingness to accept someone at his or her word. Attacking computer systems via information gained from social interactions is a form of *social engineering*. Attackers know how much easier it is to trick insiders instead of targeting the complex technological protections of systems. In an effort to formalize social engineering, we are building two models: Trust and Attack. Because social-engineering attacks are complex and typically require multiple visits and targets, these two models can be applied, individually or together, at various times to each individual attack goal.

14. SUBJECT TERMS Deception, trust, taxonomy, countermeasure			**15. NUMBER OF PAGES** 69
			16. PRICE CODE
17.SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

DEVELOPMENT OF METHODICAL SOCIAL ENGINEERING TAXONOMY PROJECT

Lena Laribee
Captain, United States Air Force
B.S., Christian Brothers University, 2001

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
June 2006

Author: Lena Laribee

Approved by: Craig H. Martell
Thesis Co-Advisor

Neil C. Rowe
Thesis Co-Advisor

Peter J. Denning
Chairman, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Since security is based on trust in authenticity as well as trust in protection, the weakest link in the security chain is often between the keyboard and chair. We have a natural human willingness to accept someone at his or her word. Attacking computer systems via information gained from social interactions is a form of *social engineering*. Attackers know how much easier it is to trick insiders instead of targeting the complex technological protections of systems. In an effort to formalize social engineering, we are building two models: Trust and Attack. Because social-engineering attacks are complex and typically require multiple visits and targets, these two models can be applied, individually or together, at various times to each individual attack goal.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

ABBREVIATIONS AND ACRONYMS

ID	Identification
IT	Information Technology

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

Without Professor Craig H. Martell and Professor Neil C. Rowe's advice and assistance this thesis would not have been possible. I greatly appreciate their gracious attitude and patience.

I would also like to thank the Office of the Secretary of Defense, Operational Test and Evaluation Directorate, and the 92nd Information Warfare Aggressor Squadron for providing the necessary data and observation experiences.

Last but not least, thank you to my husband, Trevor J. Laribee for all of his love, support, and understanding throughout this process.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

With the ubiquity of computer information processing, the deadliest security vulnerability is literally in our hands. Can we create a security patch for human nature? Unauthorized access to critical and even life-threatening data is prone to social engineering attacks, manipulation of authorized users to gain unauthorized access to a valued system and the information that resides on it. Social engineering attacks are not confined to military defense programs, day-to-day activities such as banking and paying taxes can be affected. "[This] report…reveals a human flaw in the security system that protects taxpayer data. More than one-third of Internal Revenue Service employees and managers…provided their computer login and changed their password." (Dalrymple, 2006).

A. OVERVIEW OF SOCIAL ENGINEERING

Intruders are always on the lookout for ways to gain access to valuable resources such as computer systems, or corporate or personal information on them that can be used maliciously for the attackers' personal gain. Sometimes they get their chance when there are genuine gaps in the security that they can breach. Oftentimes, they get through because of human behaviors such as trust (when people are too trusting of others) or ignorance (people who are ignorant about the consequences of being careless with information). Attackers know how much easier it is to trick insiders instead of targeting the complex technological protections that we spend huge monetary sums on. Figure 1 taken from (Hermansson, 2005) illustrates how the social engineer exploits the weakest link of a computer system, the human user, rather than directly attacking the computer hardware.

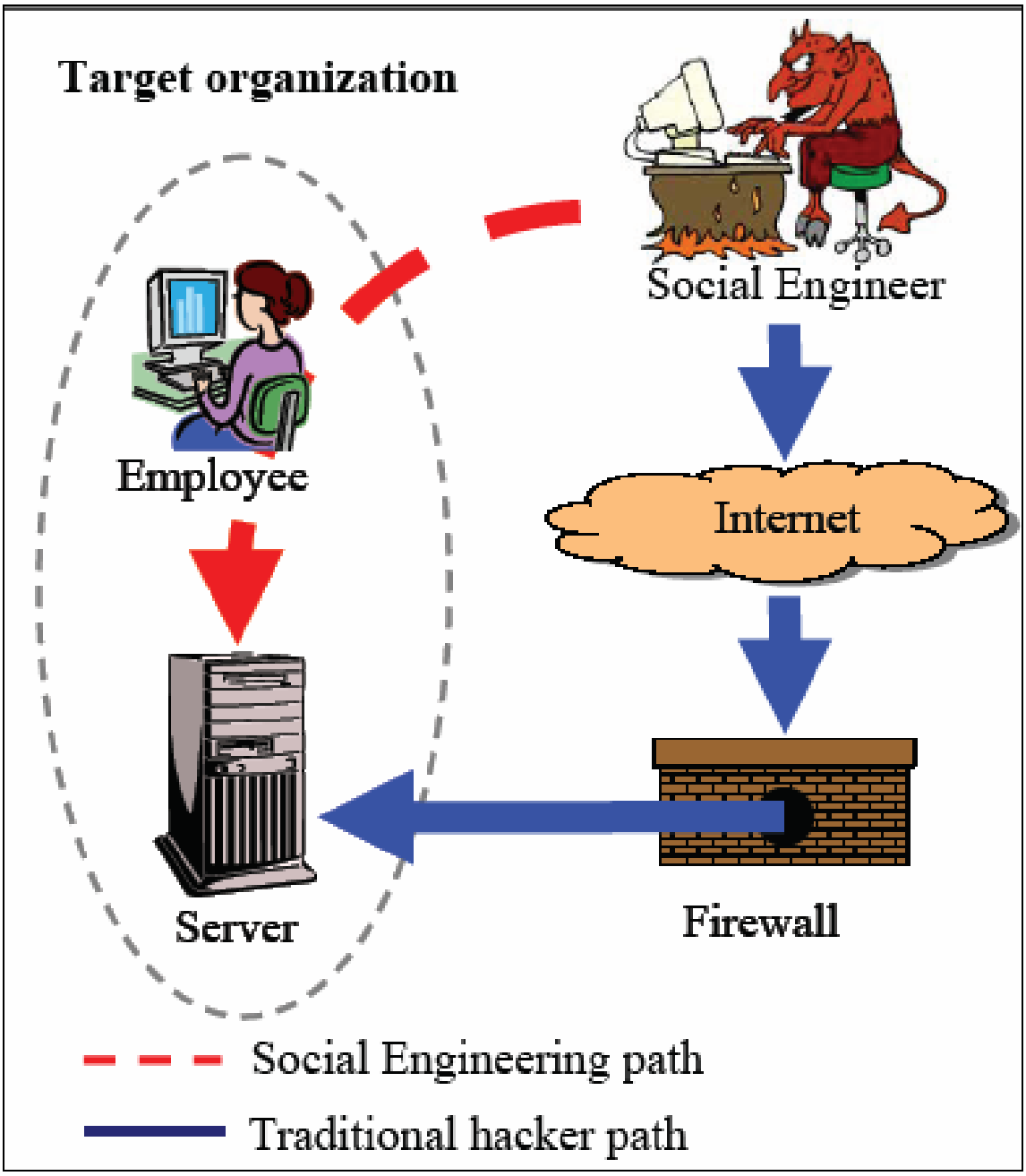

Figure 1. Why Social Engineer (From Hermansson, 2005)

There are several methods that the malicious individual can use to try to breach the information security defenses of a personal computer or a network of systems. The human-centered approach termed *social engineering* is one of them. There are two main categories under which all social engineering attempts can be classified: computer or technology-based deception, and human based deception. The technology-based

approach is to deceive the user into believing that he is interacting with a bona fide communication entity (another user, company, or website) and get him to provide confidential information. For example, the user gets a popup window, informing him that the computer application has had a problem, and the user will need to re-authenticate in order to proceed. Once the user provides their identification and password on that pop-up window, the harm is done. The attacker who has created the popup now has the user's identification (ID) and password and can access the network and the computer system. The human-based approach is done through deception, by taking advantage of the victim's ignorance and the natural human inclination to be helpful and liked. For all intents and purposes, the technology-based approach is what this thesis will refer to as *social engineering* and the human based approach as the *close access techniques*.

B. SOCIAL ENGINEERING IMPLICATIONS

Social engineering attacks can result in a network outage, fraud, identity theft, and industrial espionage. There is also the cost of loss of reputation and goodwill, which can erode a person's or company's base in the long run**.** For example, a malicious individual can get access to credit card information that an online vendor obtains from customers. Once the customers find out that their credit information has been compromised, they will not want to do anymore business with that vendor because the site is considered insecure. More directly, an attacker could initiate lawsuits against the company that will lower the target's reputation and turn away clientele. Security experts propose that as our culture becomes more dependent on information, social engineering will remain the greatest threat to any security system.

Many companies conduct safety courses and testing in order to ensure their employees are working safely and responsibly, however few companies take that same stance with information security. They neglect to remind employees about the ways "information theft" is conducted. Social engineering is an underestimated security risk rarely addressed in employee training programs or corporate security policies. (McDermott, 2005)

C. PURPOSE OF STUDY

Over the past few years of operational assessments of information assurance and interoperability, social engineering and close-access techniques have proved particularly effective at allowing Red Team and Opposing Force personnel to gain access to sensitive and secure areas, often in spite of doctrinally sound Force Protection Plans. Previous assessment showed that current tactics, techniques, and procedures with their associated training do not adequately address the social engineering and close-access threats. This research assessment will examine social engineering and close-access techniques for elements that may lead to "pattern recognition" or improved probabilities of detection. It will try to provide guidelines for policymakers in fighting the threats.

Policymakers and management, alike, must understand the importance of developing and implementing well-rounded security policies and procedures. They must understand that all amounts of money spent on software patches, security hardware upgrade, and audits will be useless without adequate prevention of social engineering attacks. Having clear-cut policies to counter social engineering attacks alleviates the employee's responsibility to make judgment calls regarding an attacker's requests. Simply, if the solicited deed is prohibited by written policy, a target employee is bound by company rules to deny the attacker's request.

D. ORGANIZATION OF PAPER

This thesis contains six chapters. Chapter II gives the background information to properly understand how social engineering works and describes its various forms. Chapter III discusses other work in the area that attempts to solve the problem. Chapter IV will propose our social engineering taxonomy, its trust and attack models, and how each model can be used for social engineering prevention. Chapter V will present our social-engineering encoding scheme and use it to analyze the cases presented in Mitnick's "The Art of Deception." Chapter VI concludes by summarizing the key issues and conclusions drawn in this thesis and postulates areas for future work.

II. BACKGROUND

In this chapter, the first section gives an outline of social engineering and its categories. The next section provides an in-depth review of close-access techniques used to obtain trust via human face-to-face interaction. The next section considers technology-based techniques. The last section discusses intelligence-gathering methods independent of human or technology focus.

A. INTRODUCTION

Kevin Mitnick, a notorious social engineer, sums it up nicely, "You could spend a fortune purchasing technology and services...and your network infrastructure could still remain vulnerable to old-fashioned manipulation." The focus of security is trust in protection and authenticity. Why is the weakest link in the security chain between the keyboard and chair? The natural human willingness to accept someone at his or her word leaves us vulnerable to intrusions of a social engineer.

The fundamental goals of social engineering are the same as computer hacking: to gain unauthorized access to systems or information in order to commit fraud, network intrusion, industrial espionage, identity theft, or simply to disrupt the system or network. The key to social engineering is knowing the jargon, the corporate infrastructure, and human nature. A good attacker exudes such confidence that few challenge him or his requests for seemingly, innocuous information. Typical targets include big-name corporations and financial institutions, military and government agencies, and infrastructure providers (hardware, software, communication, voice mail vendors). The Internet boom had its share of industrial engineering attacks in start-up companies, but attacks generally focus on larger entities with high-valued assets (Granger, 2001).

Even though any social engineering involves exploiting someone's trust, there are two main categories: a human-based approach and a computer or technology-based approach. The human-based approach is done through face-to-face communications, by taking advantage of the victim's ignorance and the natural human inclination to be helpful and liked. The technology-based approach deceives the user through electronic

communication. We will call the human-based approach the *close-access technique*, and the technology-based approach, *social engineering*.

Besides these two categories are two common methods of obtaining confidential information that are not centered on technology or face-to-face interaction: open-source research and covert searches or "dumpster diving". Although collecting open-source information on the Internet uses technology, this method does not require human manipulation.

B. CLOSE-ACCESS TECHNIQUES

Many organizations only plan for attacks directly against physical or technical resources and ignore the threat from attacks via human resources. Close-access techniques use face-to-face manipulation to gain physical access to computer systems and, ultimately, the information contained in them. We are referring to the manner in which the attack is carried out, emphasizing how to create the perfect psychological environment for the attack.

Typically, successful social engineers have great people skills. The main objective is to convince the target, a person knowing some valuable information, that the attacker is a trusted person that has a need to know. Often an attacker exploits people's ignorance of the value of the information they possess and their carelessness about protecting this seemingly innocuous data. These close-access techniques from (Granger, 2001) include: friendliness, impersonation, conformity, decoying, diffusion of responsibility, and reverse social engineering. Reciprocity, consistency, and scarcity are proposed in (Cialdini, 2001). In addition, our research adds sympathy, guilt, equivocation, ignorance, and affiliation to the set of trust ploys used to gain access and information.

1. Friendliness

A fundamental *close-access technique* to obtain information is just to be friendly. Because people tend to comply readily with individuals they know and like, any social engineer is most effective emphasizing factors that increase their overall attractiveness and likeability. The average user wants to believe their colleagues and wants to help, so

the attacker really only needs to be cordial and convincing. Beyond that, most employees respond in kind, especially to women. Often times, slight flattery or flirtation might even help soften up the target employee to co-operate further. A smile or a simple "thank you" usually seals the deal.

2. Impersonation

Impersonation means creating a character and playing out the role to deceive others and gain some advantage. The simpler the role, the better. Sometimes this could mean just calling someone up and saying: "Hi, I'm Bob in Information Technology (IT), and I need your password." Other times, the attacker will study a real individual in an organization and wait until that person is out of town to impersonate him over the phone or even in person. Industrious attackers with a high-valued target may even use an electronic device to disguise their voices and study speech patterns and organizational charts. Common roles impersonated include a repairman, an IT support person, a manager, a trusted third party, and a fellow employee. For example, someone alleging to be the CEO's secretary calls to say that the CEO okayed her requesting certain information. In a big organization, this is not that hard to do. It is difficult to know everyone, and IDs and entrance badges are easy to fake with the right tools.

We will not use impersonation as a specific attack toolkit item since it seems to be used in most close-access/social engineering attacks, with an attacker pretending to be someone or something, such as a legitimate website, to exploit the target's trust.

3. Conformity

Conformity is the tendency to see an action as appropriate when others are doing it. This close-access technique, also known as social proof, can be used to convince a target to give out information by informing him that other associates are or have been complying with the same request. When people are uncertain, they are more likely to use other's actions to decide how they themselves should act, especially if the compared individual or group is similar to the target.

4. Diffusion of Responsibility

When individuals believe that many others are present or have done a similar act, they as individuals do not bear the full burden of responsibility. When a social engineer attacks in such a way as to seemingly diffuse the responsibility of the employee giving the password away, it alleviates the stress on the employee and makes it easier for them to comply.

5. Decoys

We are human and are limited in what we can focus our attention on at any moment. A social engineer can exploit this limitation by decoys or distractions to conceal what they are truly seeking. If a target is diverted from their usual security focus, the attacker can obtain the illicit information more easily.

6. Reverse Social Engineering

A more advanced method of gaining information is when the attacker creates a persona such that employees will ask him or her for information rather than the other way around. This technique requires a great deal of preparation and research beforehand. If researched, planned and executed well, reverse social-engineering attacks offers the attacker a safe way of obtaining valuable data from the target employees since the victim is initiating transactions. The decision to comply to a reverse social-engineering sting is steered by the reciprocity rule. This compels the target to repay, in kind, what the attacker has provided as a favor.

The three phases of reverse social-engineering attacks are sabotage, advertising, and assisting (Nelson, 2001). For example, the attacker sabotages a network, causing a problem to arise. The attacker then advertises that he can fix the problem. When the attacker comes to fix the problem, he requests certain bits of information from the target employees to get what he really came for. The victims may never know that the purported problem solver was a social engineer, because their network problem goes away.

8. Commitment and Consistency

In seeking compliance, securing an initial commitment from a victim is key. People have a natural tendency to honor commitments. A savvy social engineer realizes that people are more willing to agree to further requests that are in keeping with prior commitments.

9. Scarcity

People assign more value to opportunities when they are less available. In a social-engineering attack, a target can be pressured to give out information when he thinks help from normal channels is only available for a limited time, say before close of business.

10. Authority

Several impersonation roles fall under the category of someone with authority. Historically, we are socialized with a deep-seated sense of duty to authority, because such obedience constitutes correct conduct. We readily attribute knowledge, wisdom, and power to authoritative figures, so an attacker portraying a set of these characteristics can be more convincing.

11. Sympathy

Sympathy is usually the sharing of unhappiness or suffering. Additionally, it implies concern, or a wish to alleviate negative feelings others are experiencing. An attacker eliciting that he needs help can win over a target’s sympathy, by encouraging the target to let down his guard and offer the requested information.

12. Guilt

One definition of guilt is the feeling of obligation for not pleasing, not helping, or not placating another. Additionally, it is the acceptance of responsibility for someone else's misfortune or problem because it is bothersome to see that someone suffers. A sly social engineer can convince the target that they will suffer greatly if the request is not granted.

13. Equivocation

This technique exploits a clear sentence, spoken or typed, that has two meanings. When the perceived meaning of individual words is different from that which is intended, either the whole sentence is given new meaning or it loses meaning. An equivocal statement or question starts out sounding reasonable and gets the target to agree to certain ideas or request by deliberately attempting to create uncertainty or ambiguity. After that, the meanings of key terms are changed, thus causing the victim to agree to things they would have never accepted at the beginning.

14. Ignorance

Pretending to be uninformed to manipulate a victim to give information is another popular close-access technique. A common example is the impersonation of a new company or departmental employee who does not know the processes of the new environment.

15. Affiliation

Some attackers use name dropping to establish credibility, to proclaim association with collective organizations, or suggest being in the inner circle of acceptance. This self-promotion reduces the target's suspicion of the attacker motives.

C. ONLINE SOCIAL ENGINEERING

While the art of social engineering may have been mastered before the invention of technology and computers, the Internet is a fertile ground for social engineers looking to gather valuable information. With the proliferation of poorly-secured computers on the Internet and publicly known security holes, the majority of security compromises are done by exploiting vulnerable computers. Computer attacks that do not use social engineering is commonly termed *hacking*. This is a more direct attack using hardware and software methods and programming tricks to break a security feature on the system itself. Generally, hacking requires above-average computer skills and takes much longer than simply obtaining an authorized user's ID and password.

Social engineering for online information often focuses on obtaining passwords. While the typical social engineering attempt would be to gain trust and just ask for the

password, many technical methods can also be used to gain password information without the owner's permission. An ongoing weakness that makes these attacks successful is that many users often repeat the use of one simple password on every Internet account, even their financial institutions. Several methods can gain password information.

1. Awards

Another way in which attackers can obtain personal information is through online forms that solicit information: Attackers can send out enticing offers or "awards" and ask the user to enter their name, e-mail address, and even account passwords.

2. Pop-up Windows

Pop-up windows can be installed by attackers to look like part of the network and request that the user reenter his username and password to fix some sort of problem.

3. Network Sniffing

Sniffing means examining network traffic for passwords. A person doing sniffing generally gains the confidence of someone who has authorized access to the network, to help reveal information that compromises that networks security. Then, the attacker can monitor a screen until an unsuspecting target types in their account information.

4. Email

Email can be used for more direct means of gaining access to a system. For instance, mail attachments can carry malicious software that can gather personal information without the user knowing. Trojan horses, viruses, and worms can be slipped into the e-mail body or attachments to solicit usernames and passwords.

5. Phishing

Phishing is a form of social engineering which involves using e-mail and websites designed to look like those of well-known legitimate businesses, financial institutions, and government agencies, to deceive users into disclosing their account information. These phony websites are simulations that appear to be login screens, but are not. Graphics and format can be copied from legitimate sites to make them highly convincing.

Once trust is established, a phisher tries to obtain sensitive personal, financial, corporate or network information. Many attackers target financial or retail organizations, but military targets are increasing (especially highly targeted phishing called "spear phishing"). Phishing can try to lure consumers into revealing their personal and financial data such as social-security numbers, bank and credit-card account information, and details of online accounts and passwords. A spoofed e-mail could ask you for billing information or other personal records, supposedly from a high-ranking employee. The attacker could e-mail thousands of online customers as the head of a corporation asking them to send in their passwords because some files were lost. Phishing can also be very useful to an state-level adversary for spying or sabotage.

6. Harvesting Networks

Another tactic of social engineering is to use social-network websites such as myspace.com and friendster.com to harvest freely available personal data about participants, and then use the data in scams such as fraud and money laundering.

D. INTELLIGENCE GATHERING

1. Open-Source Research

Much historical and background information can be obtained before even talking to any person by simply surfing target web sites and looking up the target on search engines such as Google. For businesses, employee e-mail addresses and phone numbers, organizational charts, executive titles, and financial information are often publicly available. Some even have pictures of executives on their website, along with their phone number and e-mail address.

2. Dumpster Diving

Dumpster diving, also known as trashing, is another popular method of collecting information without interfacing with people or technology. A huge amount of information can be collected through company or individual dumpsters. Potential security leaks in our trash include “phone books, organizational charts, memos, policy manuals, calendars of meetings, events and vacations, system manuals, printouts of sensitive data or login names and passwords, printouts of source code, disks and tapes, company

letterhead and memo forms, and outdated hardware" (Granger, 2001). Phone books can give the attackers names and numbers of people to target and impersonate. Organizational charts contain information about people who are in positions of authority within the organization. Memos provide small tidbits of useful information for faking authenticity. Policy manuals show attackers how secure (or insecure) the company really is. Calendars may tell attackers which employees are out of town at a particular time. System manuals, sensitive data, and other sources of technical information may give attackers the exact keys they need to unlock the network. Outdated hardware, particularly hard drives, can often be restored to provide all sorts of useful information.

THIS PAGE INTENTIONALLY LEFT BLANK

III. PREVIOUS MODELS OF SOCIAL ENGINEERING

Social engineering, obtaining information by human trust manipulation, has been used for centuries, but there is little formalized theory in this area. The closest research work associated is found in the area of *trust*. The first section provides a detailed assessment of the essential role that trust plays in a successful social engineering ploy and recognizes previous trust models. The second section discusses the current prevention recommendations from computer security and social engineering experts.

A. TRUST

Social engineering uses human error and weakness to gain access to a system despite the layers of defensive security controls that have been implemented via physical safeguards, hardware, and software. Since a crucial objective is to convince the person disclosing the information that the attacker is a trusted person that has a need to know, trust is an important topic to cover to fully understand a social engineer.

Trust is subjective; there may always be hidden factors, intentional or subconsciously, behind a decision to trust or not. To deal with the immense data processing of everyday life, we must use shortcuts to sort through all the information and make judgments accordingly. "Quite a lot of laboratory research had shown that people are more likely to deal with information in a controlled fashion when they have both the desire and the ability to analyze it carefully; otherwise, they are likely to use the easier *click*, *whirr* approach" (Chen & Chaiken, 1999; Petty & Wegener, 1999). This *click*, *whirr* approach is characterized by fixed-action patterns where a set of behaviors occurs in the same fashion and in the identical order, as if these patterns are recorded on tapes. "*Click* and the appropriate tape is activated; *whirr* and out rolls the standard sequence of behaviors" (Cialdini, 2001). When we are rushed, stressed, uncertain, indifferent, distracted, or fatigued, we tend to resort to shortcuts rather than extensive analysis. As a result, "much of the compliance process (wherein one person is spurred to comply with another person's request) can be understood in terms of a human tendency for automatic, shortcut responding" (Sztompka, 1999), making us vulnerable to trust manipulation.

1. Trust Definitions

Previous research on trust does not clearly differentiate among factors that contribute to trust, trust itself, and outcomes of trust (Cook & Wall, 1980; Kee & Knox, 1970). We will focus on the relationship between two parties, not necessarily two individuals, and the reasons why a trustor (trusting party) would trust a trustee (party to be trusted). The act of trust may start out as a unilateral expectation and commitment, but the trusting results in a relationship. To understand the extent to which a person is willing to trust another person, three crucial areas must be examined:

1. the trustor's propensity to trust;
2. the trustor's perception of the trustee's benevolence, reputation, performance, and appearance; and
3. the environment circumstances.

a. Relationship

According to Sztompka, trust is a bet about the future contingent actions of others. Trust results from the idea of individual freedom; one person does not have direct control over others. In general, people have choices and are not confined to another person's dictates. The more available options people face, the less predictable are the decisions they take. But relationships between people limit the options to those acceptable to others..

b. Trustor

Trust liberates and mobilizes human agency, and releases creative, uninhibited, innovative, entrepreneurial activisms toward other people (Luhmann, 1979). Traits of the trustor will determine how easily that individual will trust another party. This measure of a person's *willingness* to trust is known as *propensity to trust*. The crucial problem for the trustor is the lack of sufficient information on all relevant aspects of the situation. Since the estimate of the potential gain or loss is not easily predicted, risk comes into play. This risk-taking opens the door for a social engineer to exploit.

c. Trustee

An attacker must appear trustworthy to the target victim, the trustor. We recognize four factors (Sztompka, 1999 & Mayer, 1995) that affect an attacker's perceived trustworthiness: benevolence, reputation, performance, and appearance. Trustworthiness correlates with the motivation, or lack of, to lie. Benevolence signifies this motivation of the trustee toward the trustor, i.e. good or bad intentions. Reputation refers to past deeds such as affiliation. Performance refers to present conduct such as the trustee's current position or job title. Appearance refers to external features, dress, actions, and worldly possessions (or lack of). Last but not least, environment is discussed in the next section at length because it is not an internal characteristic of the trustee. The higher the trustee's benevolence, reputation, performance, and appearance, the more likely the trustor would comply to a request of the trustee, the social engineer.

d. Environment

In the arena of social engineering and trust building, the situational circumstance plays a vital role in how the attacker convinces the trustor of his trustworthiness. This circumstance includes the level of information asked for, the knowledge of its value, and the state of mind of the trustor. "The trustor's perception and interpretation of the context of the relationship will affect both the need for trust and the evaluation of trustworthiness" (Mayer, 1995). This adaptability of an attacker's tactics is what makes a social engineering attack dynamic, making prevention methods harder.

e. Risk

Risk, or having something vested in an outcome, is a requisite to trust (Deutsch, 1958). "A specific quality of exchange involving trust is the presence of basic uncertainty or risk." (Sztompka, 1999) Trust is inversely proportional to the perceived uncertainty or risk involved. As our trust in an attacker increases, the risk they pose to us decreases, making us more prone to comply with their wishes. An example of this inverse relationship often occurs in situations involving female social engineers because society perceives women to be less harmful, i.e. less risky, than men.

f. Culture

Our globalizing society fosters interdependence so people must depend on others, sometimes strangers, in various ways to accomplish their personal and professional goals. Due to massive migrations, tourism, and travel we encounter and are surrounded by much diversity. Trust encourages tolerance, acceptance of strangers and recognizes differences as acceptable. Additionally, trust is a good strategy to deal with the anonymity and complexity of institutions, organizations, technological systems, and the increasingly global scope of their operations. The need for trust grows as networks become more complex (Luhmann, 1979). Trust is culturally functional because it encourages sociability, participation, and fosters a feeling of order and security.

g. Internet

Social engineering capitalizes on people's inability to keep up with a culture that relies heavily on information technology. Online transactions including banking and shopping eliminate direct human contact. The businesses realize that there is no e-business without trust. This proportional relationship between trust and information-sharing brings another point to why we are becoming increasingly prone to social engineering attacks.

> Our modern era, often termed The Information Age, has never been called The Knowledge Age. Information does not translate directly into knowledge. It must first be processed-accessed, absorbed, comprehended, integrated, and retained (Sztompka, 1999).

As a result, the shortcut measures of trust (benevolence, appearance, performance, reputation, and situation) are increasingly more vulnerable to exploitation.

2. Previous Trust Models

a. An Integrative Model of Organizational Trust

(Mayer, 1995) proposes that trust is the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party. Their model incorporates the dynamic nature of trust with the feedback loop from the “Outcomes” to the perceived characteristics of the trustee. The

outcome of the trusting behavior will influence trust indirectly through the perceptions of ability, benevolence, and integrity at the next interaction.

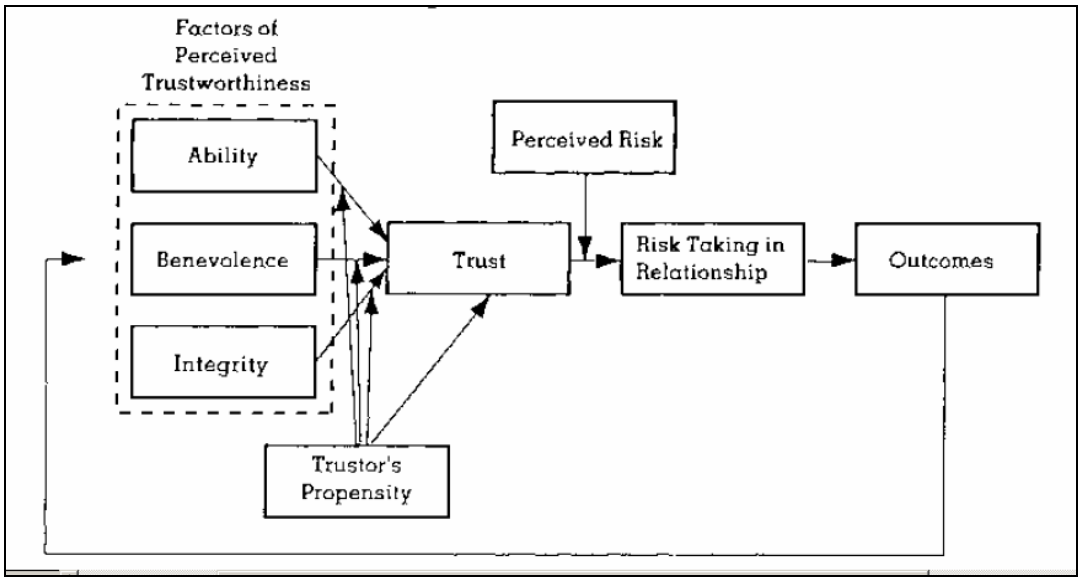

Figure 2. Integrative Model of Organizational Trust (From Mayer, 1995)

In Figure 2, the model explicitly considers both characteristics of the trustee as well as the trustor. It differentiates trust from its outcome of risk-taking in the relationship. Additionally, this model distinguishes between factors that cause trust and trust itself. They recognize that there is a need to measure the willingness to be vulnerable because trust is this willingness. As a result, this model illuminates that the level of trust of one individual for another and the level of perceived risk in a situation will lead to risk taking in the relationship.

b. Trust in Virtual Teams: Towards an Integrative Model of Trust Formation

The model from (Hung, 2004) examines the three possible routes to trust: the peripheral route, the central route, and the habitual route. In Figure 3, the three routes to trust represent the gradual shift of bases for trust formation over time as one gains personal experience and knowledge of the involved parties. While prior models describing different forms of trust emphasize trust observed at different points in time, this model integrates the different forms of trust and focuses on the dynamic shifts of trust over time by using a fundamental theoretical framework.

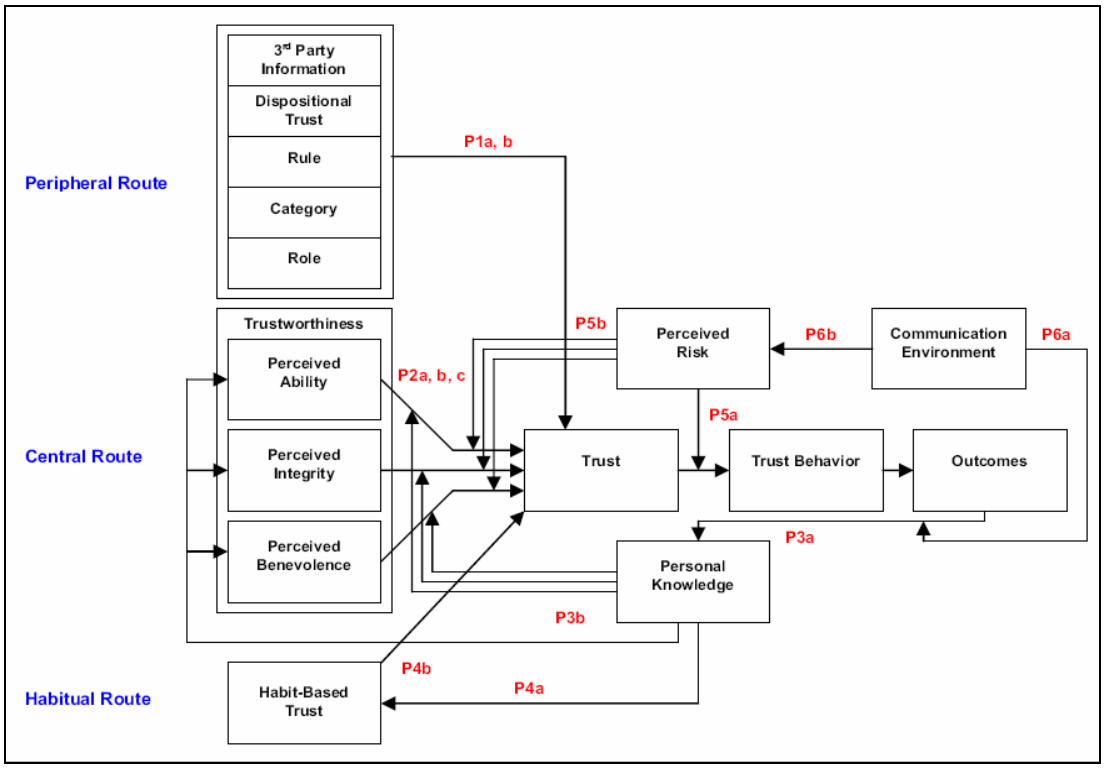

Figure 3. Trust Formation in Virtual Teams (From Hung, 2004)

c. A Distributed Trust Model

In another model, (Abdul-Rahman, 1997) highlights the need for effective trust management in distributed systems, and proposes a distributed trust model based on *recommendations*. A *Recommendation* is a communicated trust information which contains reputation information. Each agent stores reputation records in its own private database and uses this information to make recommendations to other agents. They define trust as "a particular level of the subjective probability with which an agent will perform a particular action, both before [we] can monitor such action (or independently of his capacity of ever to be able to monitor it) and in a context in which it affects [our] own action" (Gambetta, 1990). Their four goals were:

1. To adopt a decentralized approach to trust management.
2. To generalize the notion of trust.
3. To reduce ambiguity by using explicit trust statements.

4. To facilitate the exchange of trust-related information via a recommendation protocol.

B. PREVIOUSLY PROPOSED COUNTERMEASURES

Since social engineering is an attacker's manipulation of the natural human tendency to trust, prevention requires education and constant vigilance. Even though the threat is common, it is possible to keep morale high and have a mostly-trusting organization culture without sacrificing security. There are existing prevention methods and countermeasures that can be incorporated into day-to-day business. By slightly changing the rules of the daily operations and having organization-wide buy-in of its importance, social engineering attacks can be made far less often successful.

1. Admittance

Prevention starts with problem realization and is dependent on educating people about the value of information, training them to protect it, and increasing people's awareness of how social engineers operate. The importance of training employees extends beyond the Help Desk, across the entire organization. Most users should know not to send passwords in clear text (if at all), but occasional reminders of this simple security measure from the System Administrator is essential. System administrators should warn their users against disclosing any account or personal information in any fashion other than a face-to-face conversation with a staff member who is known to be authorized and trusted (Granger, 2001).

2. Recognition

To foil an attack, it helps to recognize a social engineering ploy. "Look for things that don't quite add up." (Granger, 2002) Several signs that you are dealing with a social engineer:

a) refusal to give contact information;

b) rushing;

c) name-dropping;

d) intimidation;

e) small mistakes (misspellings, misnomers, odd questions); and

f) requesting forbidden information.

3. Contingency Planning

In the event that an employee detects something suspicious, he or she needs to follow procedures in place for reporting the incident. It is important for one person to be responsible for tracking these incidents. Also, that employee should notify others who serve in similar positions as they may be threatened as well (Granger, 2002).

4. Proactive Security

Avoiding the social-engineering threat requires organizations to become more security-centric, or ensure they have a strong information security policy. The following suggestions are commonly made:.

a) Conduct ongoing in-depth information-security training.

b) Be suspicious of unsolicited e-mail messages, phone calls, or visits from individuals asking about employees or other internal information. If dealing with an unknown person claiming to be from a legitimate organization, verify their identity directly with the organization..

c) Never be afraid to question the credentials of someone claiming to work for your organization.

d) Install and maintain firewalls, anti-virus software, anti-spyware software, and e-mail filters.

e) Pay attention to the URL of a web site. Malicious web sites generally look identical to a legitimate site, but the URL may use a variation in spelling or a different domain.

f) Don't send sensitive information over the Internet before checking a website’s security.

g) Don't reveal personal or financial information in e-mail, and do not respond to e-mail solicitations requesting this information. This includes following links sent in e-mail.

h) Don't provide personal information or information about your organization to anyone, including the structure of your networks, unless you are certain of a person's authority to have that information.

i) Be careful about what is provided on your organization's web site. Avoid posting organizational charts or lists of key people like officers.

j) Shred any document that is discarded that may contain sensitive data.

k) Don't allow employees to download from anywhere (McDermott, 2005).

C. SUMMARY

Because of technological advances, information available to people is burgeoning, choices are increasing, and knowledge is exploding. These factors often make careful assessment of all information-access situations impractical. The feeling of familiarity breeds trust, providing the feeling of security, certainty, predictability, and comfort. Personnel often turn to a shortcut approach to make compliance decisions, using a single (typically reliable) piece of information. The most reliable and therefore, most popular such single triggers are the *close access techniques* described in Chapter II. Social engineers that infuse their requests with one or more of these *techniques* are more likely to get the information that they are after.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. A MODEL OF SOCIAL ENGINEERING

A. INTRODUCTION

Social engineering attacks can be very dynamic and often vary widely depending on the attacker, target information, victim, and environmental circumstances.

> [A] group of strangers walked into a large shipping firm and walked out with access to the firm's entire corporate network. [They] obtain[ed] small amounts of access, bit by bit, from a number of different employees. First, they did research about the company for two days before even attempting to set foot on the premises (Granger, 2001)

By asking the right questions, the attackers pieced together enough information to aid in their infiltration of an organization's network. If an attacker were not able to gather enough information from one source, they would contact another source within the same organization and rely on the information from the first source to add to their appearance of credibility. This continues until the attackers have enough in their toolkit to access the network and obtain the targeted data.

We propose two models, a trust model and an attack model, for what a social engineer does before, during, and after an attack. The attack model is recursive because typical attacks require more than one looping of the steps to achieve the end goal. The attack model can call on the trust model to provide the attacker another conquered information source, direct or indirect.

B. TRUST MODEL

As shown in Figure 4, our Trust Model describes how a social engineer establishes a trustworthy relationship with a person that has needed information for a social engineering attack. Initially, an attacker obtains background information (freely available if possible) about the target. A key early stage in the trust process is the receiver's (victim's) judgment of the credibility of the information provided by the attacker. From Chapter III, three prevalent areas stand out that explain trust:

1. the trustor's propensity to trust;
2. the trustor's perception of the trustee's benevolence, reputation, performance, and appearance; and
3. the environmental circumstances.

Detailed explanations of these three areas are given in Chapter III, A. I. Trust Definitions. Traits of the trustor will determine how easily that individual will trust another party. This is known as *propensity to trust*. The surrounding *environment* plays a vital role in convincing the trustor that the attacker is trustworthy. Environmental factors include the level of information being requested, the trustor's knowledge of it's value, and the trustor's state of mind.

Trustworthiness correlates with the motivation, or lack of, to lie. We recognize four factors (Sztompka, 1999 & Mayer, 1995) that affect an attacker's perceived trustworthiness: benevolence, reputation, performance, and appearance. Benevolence signifies this motivation of the trustee toward the trustor, i.e. good or bad intentions. Reputation refers to past deeds and affiliations. Performance refers to present conduct such as the trustee's current position or job title. Appearance refers to external features, dress, actions, and worldly possessions (or lack thereof). Source (trustee or receiver), trustor, and the circumstances surrounding the attack all interact in the assessment of trusting. Presenting some combination of these character traits and manipulating the others, the trustee convinces the target that he is a trusted person that has a need to know.

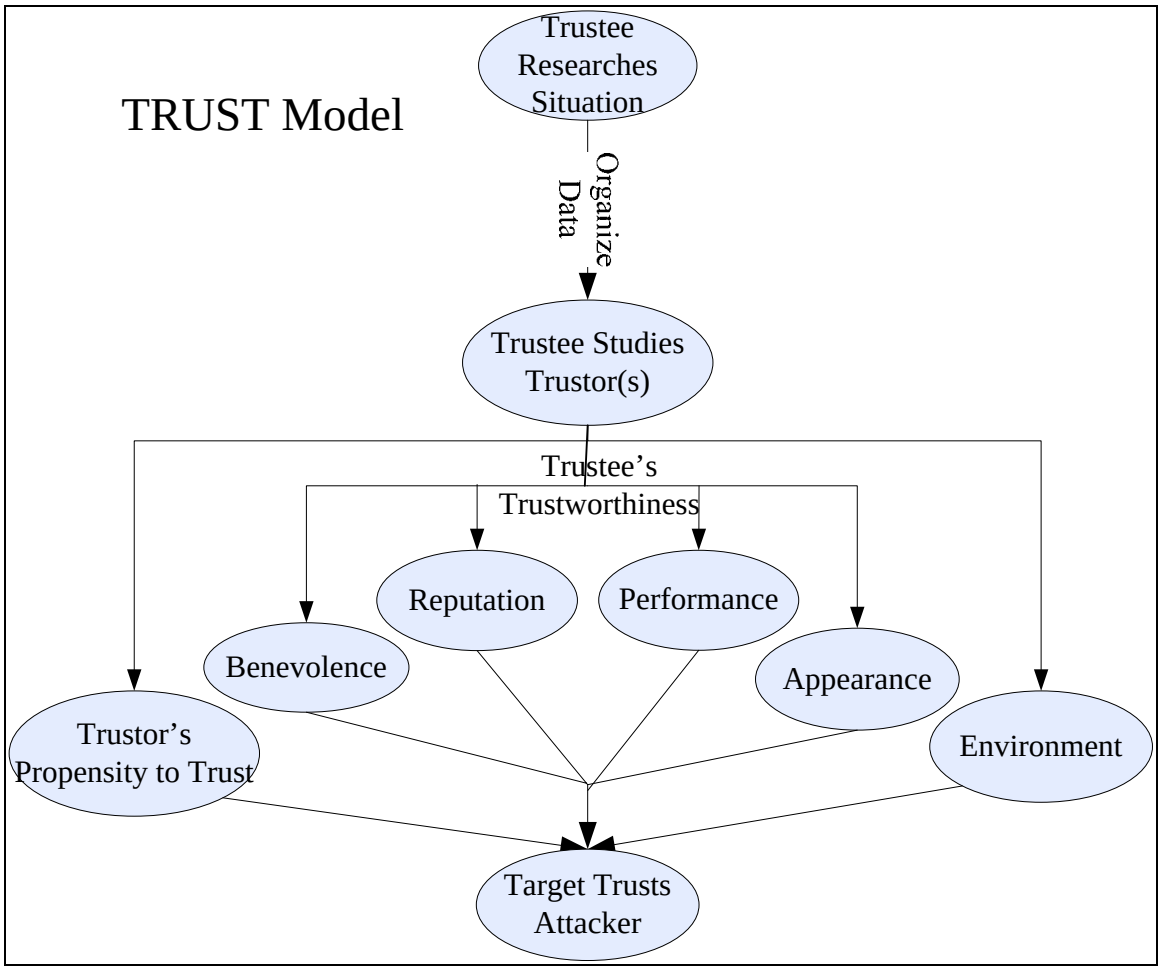

Figure 4. Social-Engineering Trust Model

C. ATTACK MODEL

Our Attack Model illustrates how a single typical information-gathering attack is carried out to obtain a single item of information, a kind of "subroutine" for a class of social-engineering ploys. Here the connections between nodes represent actions. Trust of a victim by an attacker is usually developed with the methods of the Trust Model as a precondition to most of the steps of the Attack Model. The model begins when the social engineer undertakes some research on the target individual or organization. The information gained, even if not helpful, may be used to obtain further information that might be helpful. Then the attacker uses one of a number of techniques to achieve their objective.

In Figure 5, there are four main categories of attack techniques. They are deception, causing to believe what is not true; influence, to sway or affect based on prestige, wealth, ability, or position; persuasion, to induce to undertake a course of action by means of argument, reasoning, or entreaty; and manipulation, to falsify for malicious gain. The toolkit of a social engineering attack includes the tactics of friendliness, conformity, decoying, diffusion of responsibility, reverse social engineering, consistency, scarcity, sympathy, guilt, equivocation, ignorance, and affiliation. Using some combination of these trust ploys to achieve one or more of these attack techniques, the social engineer tries to gain unauthorized access to systems or information. The intent is usually to commit a crime such as fraud, espionage, identity theft, or vandalism of a system or network. Depending on the size and other characteristics of the target information, the Attack Model can recurse until the goal is achieved.

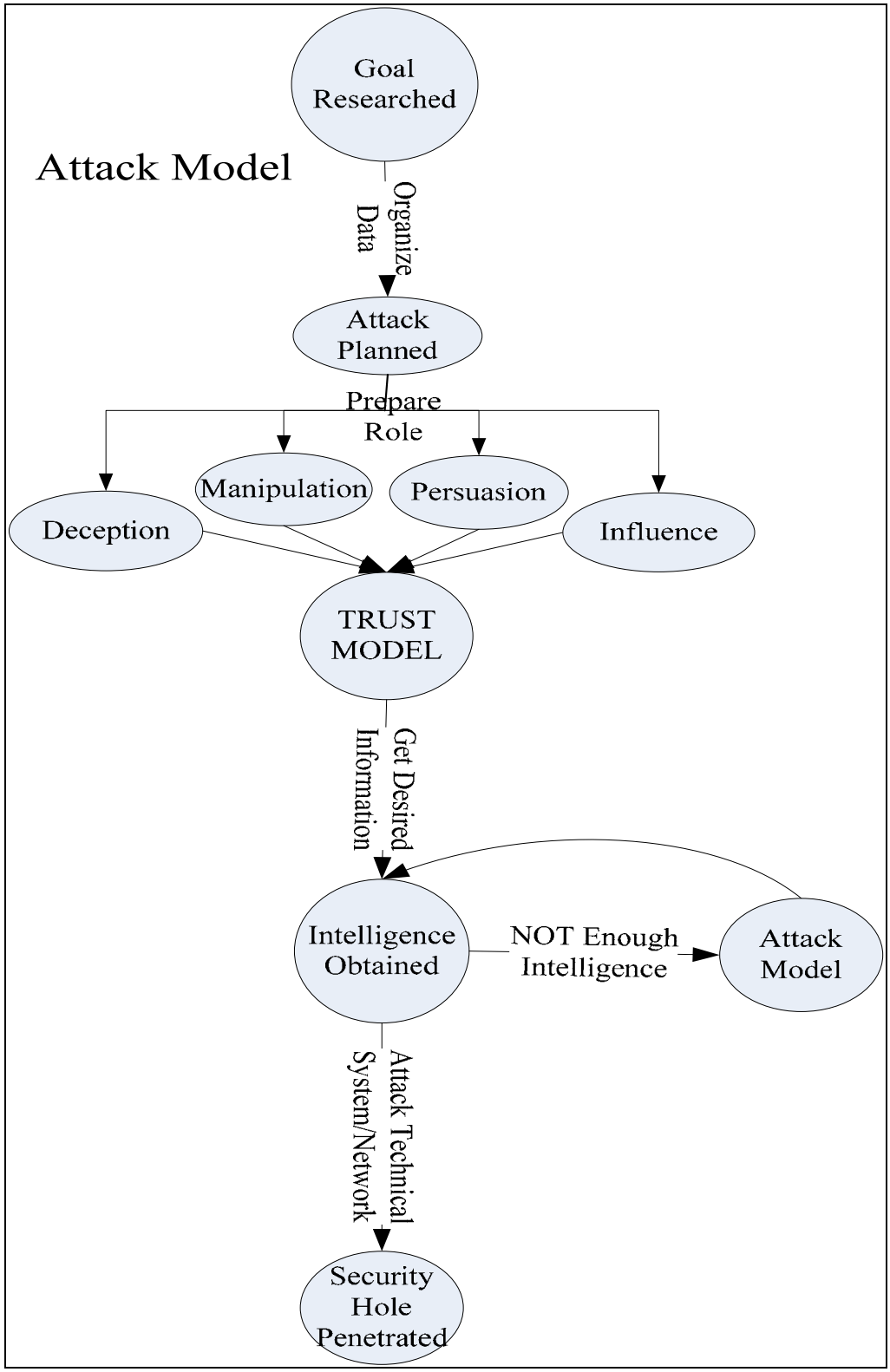

Figure 5. Social-Engineering Attack Model

THIS PAGE INTENTIONALLY LEFT BLANK

V. TAXONOMY APPLIED TO MITNICK'S EXAMPLES

A. INTRODUCTION

We can use the models given in Chapter IV, plus the taxonomies discussed in Chapters II and III, to better characterize the anecdotes of social-engineering attacks given in (Mitnick, 2002). Assessing an attack with this encoding will enable us to pinpoint areas of improvement or focus our attention on the most vulnerable spots that a social engineer relies on.

B. OUR TAXONOMY FOR ENCODING SOCIAL ENGINEERING ATTACKS

We propose four main dimensions of interest in determining the type and severity of a social engineering attack. Our goal is to find the holes and propose countermeasures or prevention techniques. The first category is the *Target* of interest:

a) Finance (banks, credit card vendors, credit agencies)
b) Commercial
c) Government
d) Infrastructure provider (hardware, software, communications)
e) Infrastructure

The second category is the *Type of Deception* from the associated semantic case or set of cases in (Rowe, 2006):

Space:

1) Direction, of the action
2) Location-at, where something occurred
3) Location-from, where something started
4) Location-to, where something finished
5) Location-through, where some action passed through
6) Orientation, in some space

Time:

7) Frequency, of occurrence of a repeated action
8) Time-at, time at which something occurred
9) Time-from, time at which something started

10) Time-to, time at which something ended
11) Time-through, time through which something

Participant

12) Agent, who initiates the action
13) Beneficiary, who benefits
14) Experiencer, who senses the action
15) Instrument, what helps accomplish the action
16) Object, what the action is done to
17) Recipient, who receives the action

Causality:

18) Cause
19) Contradiction, what this action opposes if anything
20) Effect
21) Purpose

Quality:

22) Accompaniment, an additional object associated with the action
23) Content, what is contained by the action object
24) Manner, the way in which the action is done
25) Material, the atomic units out of which the action is composed
26) Measure, the measurement associated with the action
27) Order, with respect to other actions
28) Value, the data transmitted by the action (the software sense of the term)

Essence:

29) Supertype, a generalization of the action type
30) Whole, of which the action is a part

Speech-act theory:

31) External precondition on the action – inserting precondition when non-existent
32) Internal precondition, on the ability of the agent to perform the action – new hire employee

The third category is the particular *Resource or Target Information*:

A) Identification – password/internal code, username, employee #/ID

B) Affiliation status - entrance badge, other company employees

C) Internal information – contact information, authority name(s), account information, process information, work schedule, organizational chart, company directory, hardware/software/application information, access procedure

D) Data/product movement/change/software install/hardware install

E) Trust

The fourth category is the *Trust Ploy* taken from Chapter II:

i) Reverse social engineering

ii) Commitment/Consistency

iii) Authority

iv) Friendliness

v) Scarcity

vi) Conformity

vii) Sympathy

viii) Guilt

ix) Diffusion of Responsibility

x) Decoy

xi) Equivocation

xii) Ignorance

xiii) Affiliation

C. ENCODING OF THE MITNICK ANECDOTES

(Mitnick, 2002) is a classic summary of social-engineering techniques, but its anecdotal nature makes it hard to infer principles of social engineering from it. So we encoded each of the anecdotes using our taxonomy, described in the previous section, in order to better see patterns. As an example, we will encode the Swiss Bank Anecdote using the four main dimensions of interest in determining the type of social engineering attack.

1) Swiss Bank Account, pg 4: target – a

   a) Obtain daily code: 21Ax,xii

   b) Request transfer: 12Dvi

Since the goal was to get $10, 200, 000 wired to a Swiss bank account, the Target dimension is encoded as (a) for Finance. There are two information-gathering objectives required for the end-goal to be achieved. First, the social engineer needs to obtain the daily code to authorize the wire transfer. To obtain the code, the attacker impersonated an IT staff member who needed to look at the operating procedures for the back-up system of the wire room. This is entails deception of Purpose, (21) in our encoding. The (A) signifies that the Target Information was Identification. The Trust Ploys used in this objective were Decoying, distracting the employees in the wire room with his deceptive purpose, (x), and Ignorance, exploiting the employee's thinking that the daily codes are unimportant in that they were posted out in the open, (xii).

Second, the social engineer must request the wire transfer of money. The social engineer used deception of Agent, (12), because he represented himself to the bank representative as an employee in the bank's International Department. The Target Information in this objective was the movement of money, electronically which we encoded as (D). The Trust Ploy that the social engineer exploited in this attack is Conformity in that the bank representative simply did what she thought was regular daily operations, (vi).

Below are the encodings for the rest of the Mitnick examples.

2) Creditchex, pg 16: Creditchex concerns a private investigator's obtaining credit information of a husband that left his wife, taking all their savings.

   Target: a

   a) Get industry terminology: 21Eiv,xii
   b) Obtain current merchant ID: 21Cx,xii

3) Engineer Trap, pg 22: Engineer Trap explains how an employment agency seeks out qualified, already employed electrical engineers for a start-up company.

   Target: b

   a) Get Accounts Receivable contact #: 21Cii,iv,xii
   b) Get cost center #: 21Cii,iv,x,xii
   c) Get dept to call for directory: 12Biv,vii,x,xii
   d) Obtain directory mailed: 21Dii,iv,x

4) Obtain employee #, pg 26: This anecdote describes how to obtain a valid employee number by claiming a clerical error exists. (d12Aiv,x,xii)
5) Obtain unlisted contact #, pg 31: To obtain a non-published number, simply pose as an overworked fellow employee needing a little help to accomplish a heavy-duty assignment in the field. (d12Civ,vii,x,xii)
6) State talk to FBI database, pg 33: This illustrates how a social engineer finds out if the state department communicates with the FBI for hiring. (c12Cx)
7) Obtain Test Number Directory, pg 35: The story tells how one would go about obtaining a prized directory listing telephone numbers used by phone technicians. (d21Cix,xii)
8) Obtain customer information, pg 36: To obtain personal information on a customer of a gas company, simply pose as a co-worker without computer access due to a malicious software attack. (d21Cii,iv,vii,xii)
9) Video Store, pg 42: This illustrates how easy it is for a social engineer to obtain your credit card information from a video store over the telephone.

    TargetT – a

    a) Get store manager info: 21Biv,vi,xii
    b) Obtain credit card info: 12Cii,iii,iv,vi,vii

10) Calling plan, pg 48: This story explains how an attacker obtained a free cell phone from a store representative.

    Target - b

    a) Get employee schedule: 21Biv,vi
    b) Obtain phone for free: 12Ciii,iv,vi,vii

11) Network Outage, pg 55: This example of reverse engineering shows the steps for making a victim ask the attacker for IT help.

    Target – e

    a) Get port #: 12Ci,iii,iv,vi
    b) Cause network outage: 21Eiii,vi
    c) Requests help from target: 18Ei,iii,vi
    d) Download malware: 18Diii,ix

12) Who's new, pg 61: This anecdote describes the simple steps to obtain the names of new employees. (d21Ciii,iv,vi)
13) Obtain password, pg 62: This encoding illustrates how a social engineer poses as a helpful IT staff member to gather authentication credentials from unsuspecting users. (e21Ai,iii,iv,vi)
14) Proprietary information, pg 65: Some attacks are more involved than others. This anecdote discusses the steps taken to get an account with privileged access.

    Target - e

    a) Get associated people's info: 21Biv,vi,xii
    b) Get computer system's name: 12Ciii,vi,xii
    c) Obtain names and e-mails faxed: 21Ciii,vi,xii
    d) Get external dial up #: 12Cvi,vii
    e) Get a password from UNIX's hashed file: n/a
    f) Obtain authorized username and password: 21Ai,iii,v,vi,vii,viii,x

The next two social engineering attacks, 15 and 16, describe how to gain access to anan organization's internal network.

15) WAN access, pg 77: target – d
    a) Get employee name from receptionist: 22Axii
    b) Get employee number: 18Ax
    c) Obtain dial up access: 12C "asked for it"
16) Encryption software, pg 85: target – d
    a) Get Secure ID token access: 12Aix,xiii
    b) Get servers' names: 12Cvi
    c) Obtain Telnet access: 12Cxiii
17) Update account for $5, pg 97: Five dollars is a trivial amount, but this story shows how it can lure a user into giving away their personal account information. (a29Cx,xii,xiii)
18) Getting on the A-list, pg 106: This illustrates how easy it is to obtain entrance credentials for a movie studio. (b32Biv,vii,xiii)

19) Getting cheating ex's unlisted number, pg 108: Being female, friendly, and knowledgeable about industry "lingo" will get you many things, including an ex-boyfriend's unlisted telephone number. (d21Ciii,x)
20) Need report yesterday, pg 111: This describes the affects of using authoritative intimidation to obtain a proprietary report. (e31Diii,xiii)
21) Public servant in need, pg 112: This story shows that government systems can be attacked by exploiting sympathy and people's willingness to help. (c18Bvii,xiii,iv)
22) Lucky Monday, pg 117: This describes how a helpful social engineer gets an unsuspecting employee to change her password just long enough for him to get access using her account information. (e19Di,iii,iv,xiii)
23) Am I wanted, pg 121: This story tells how a criminal finds out if there is a warrant out for his arrest.

    Target - c

    a) Get warrant: 21Cxiii,iii,vi,vii
    b) Reroute fax: 13Cxiii,vi,vii

24) Stealing a degree, pg 125: Identity theft is shown in this story; the attacker steals personal information from a graduate that shares his name.

    Target - e

    a) Get server name: 12Ciii,xiii
    b) Get authorized username and password: 21Axii
    c) Get database procedure: 18Cvii,xiii

D. SUMMARY STATISTICS

For our summary statistics, we list the total counts of occurrences for each item.

Target of interest: Throughout (Mitnick, 2002), we assessed 24 targets of interests.

a) Finance - 4
b) Commercial - 3
c) Government - 3
d) Infrastructure provider - 8
e) Infrastructure - 6

Type of Deception: Among the 24 targets of interest, there were 45 instances of deception steps that warrant labeling.

Space:

1) Direction, of the action - 0
2) Location-at, where something occurred - 0
3) Location-from, where something started - 0
4) Location-to, where something finished - 0
5) Location-through, where some action passed through - 0
6) Orientation, in some space - 0

Time:

7) Frequency, of occurrence of a repeated action - 0
8) Time-at, time at which something occurred - 0
9) Time-from, time at which something started - 0
10) Time-to, time at which something ended - 0
11) Time-through, time through which something - 0

Participant

12) Agent, who initiates the action - 15
13) Beneficiary, who benefits - 1
14) Experiencer, who senses the action - 0
15) Instrument, what helps accomplish the action - 0
16) Object, what the action is done to - 0
17) Recipient, who receives the action - 0

Causality:

18) Cause - 5
19) Contradiction, what this action opposes if anything - 1
20) Effect - 0
21) Purpose - 19

Quality:

22) Accompaniment, an additional object associated with the action - 1
23) Content, what is contained by the action object - 0
24) Manner, the way in which the action is done - 0
25) Material, the atomic units out of which the action is composed - 0
26) Measure, the measurement associated with the action - 0

27) Order, with respect to other actions - 0

28) Value, the data transmitted by the action - 0

Essence:

29) Supertype, a generalization of the action type - 1

30) Whole, of which the action is a part - 0

Speech-act theory:

31) External precondition on the action - 1

32) Internal precondition - 1

Resource or Target Information: Each of the 45 instances of labeled deception steps are accompanied by corresponding target information.

A) Identification - 8

B) Affiliation status - 6

C) Internal information - 23

D) Data/product movement/change/software install/hardware install - 5

E) Trust - 3

Trust Ploy: Because each attack step can use any combination of close access techniques, each of the 45 instances of labeled deception steps are accompanied by various sets of trust ploys.

i) Reverse social engineering - 5

ii) Commitment/Consistency - 5

iii) Authority - 15

iv) Friendliness - 16

v) Scarcity - 1

vi) Conformity - 18

vii) Sympathy - 12

viii) Guilt - 1

ix) Diffusion of Responsibility - 2

x) Decoy - 12

xi) Equivocation - 0

xii) Ignorance - 17

xiii) Affiliation - 11

E. COUNTERMEASURES FROM EXPERIMENT

Within the Target category, the Infrastructure Provider was the most targeted institution. This is only logical from a social-engineering standpoint because attackers need insider information; the bulk of an attack is gathering enough background information to be reputable. Infrastructure providers often hold the key to intermediary access. The key to attack prevention within these companies is awareness. On-going, relevant education about social engineering vulnerabilities must be enforced as a critical company policy that is supported throughout—from CEO down to line employees. More about this prevention method is presented in Chapter IV.

Among the Types of Deception, deception of *Agent* and deception of *Purpose* are the most prevalent. "Identification of participants responsible for actions ('agents') is a key problem in cyberspace, and is an easy target for deception. Deception in…purpose… is important in many kinds of social-engineering attacks where false reasons like 'I have a deadline' or 'It didn't work' are given for requests for actions or information that aid the adversary (Rowe, 2006)". Since recognition is the first step to prevention, multimodal training must be implemented to help employees recognize a social engineer via an understanding of typical personae and the reasons commonly used to obtain illicit information from authorized users. Multimodal training includes interactive computer case-studies, live acting of scenarios, picture(s) of phishing e-mails and phony websites, and audio clips of what a social engineer would sound like over the phone. Similarly to how firefighters are trained for their life-saving jobs, employees must realize that a social-engineering attack can result in a fatality by leaking classified information about national security.

In the *Target Information* category, attacks to gain Internal-Information are the most common. Similar to how Infrastructure Providers are the center of attention among institutions; this class of information is most vulnerable to attack due to its value in fostering trust and reputation for a social engineer.

Finally, Conformity and Ignorance are the traits most susceptible to a social–engineering attack. The natural human tendency to do as others do, combined with the notion that the information they possess is innocuous, can be dangerous when exploited

by an attacker seeking prohibited information. Having policy ingrained into everyday operations will lessen the burden of targeted victims to make decisions when under attack by a preying social engineer. Additionally, awareness and multimodal training may effectively counter Internal Information, Conformity, and Ignorance risks. The key is defense in depth with organization-wide buy-in and participation.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION AND FUTURE WORK

With our ever-increasing dependence on rapidly advancing technology, there is no single method that will fully protect against security threats, especially social-engineering threats. It is harder to protect yourself against social engineering than against malicious software attacks. Since social-engineering is not as predictable as a virus outbreak, it is important to always keep in mind that it can strike anybody at any time. Additionally, software has limited ways to execute while a social engineer can attack from many different angles. Fortunately, there are ways to reduce the possibility of successful social-engineering attacks. Defense-in-depth with constant vigilance and multimodal training, coupled with strong policy, will usually be the best defense strategy.

A. RECOMMENDATIONS FROM EXPERIMENT

We have presented a taxonomy that should be useful for modeling and assessing a social-engineering attack. Based on the two models, Trust and Attack, we propose these actions to harden security in their specific areas.

Given the Trust Model, initial prevention methods can be taken at the step where the Trustee Researches and Studies the Situation and Trustor. An organization should be particularly careful about what is provided on the organization's or personnel's websites. Posting organizational charts or lists of key personnel and computer administrators should be avoided. Also, any document that is discarded that may contain proprietary, sensitive, or personal data should be shredded.

When the trustee's trustworthiness is in question, i.e. an information requester that is slight suspicious, personnel should never provide personal information or information about the organization, including the structure of your networks, to anyone unless that person's authority to have that information is verified. Unsolicited e-mail messages, phone calls, or visits from individuals asking about employees or other internal information should be treated as suspicious. If dealing with an unknown person claiming to be from a legitimate organization, verify their identity directly with that organization.

In the attack model, the steps represented with a circle are focus areas where preventive measures and awareness can lessen the chances for a successful social-

engineering attack. At Goal Researched, similar preventive steps to those mentioned above that will help keep information away from the attacker are recommended. Before the implementation of the Trust Model to obtain needed trust from the victim, recognition tactics would help prevent would-be victims from believing deceptions so readily. One tactic would be to focus on signs that the requester has harmful intentions, e.g. the refusal to give contact information, rushing, name-dropping, intimidation, requesting odd information, and uncommon flattery. Additionally, security policy should somehow be automated so that the guesswork and decision-making responsibility is removed from the human victim. To counter a social engineer from Technically Attacking the System or Network, encryption, intrusion-detection tools and auditing of account access will help prevent a hacker from gaining access or slow him down long enough to allow system administrators can fight them directly.

B. CONSTANT VIGILANCE

In addition to the countering techniques developed from the modeling of social engineering, one of the most effective countermeasures is having well-educated, security-conscious employees. All employees throughout the organization need to be aware of the risks and remain vigilant (Barber, 2001). The security policies and procedures should be taught to every new employee and repeated periodically for the entire organization. To repeatedly train employees is important to keeping their social-engineering awareness at a constant, high level.

Stolen data could result in company closure and many unemployed personnel. When educating employees, it is not sufficient to simply tell them how they should behave. It is essential that they are aware of the reasons for the education and fully believe in the value of the time and effort put forth. This is the reason employee buy-in is necessary to maintain a security-motivated team. All employees must understand why they should behave in a certain way. It is critical that management, as well as the rest of the organization, fully recognize and appreciate the awareness program. There is no substitute for knowledgeable employees that realize the interdependency of their everyday actions with those of the rest of the organization.

Since social engineers can attack any employee when attempting to gain illicit information, *all* employees should understand the social engineer's methods of attack and

be aware of whom to trust when a problem occurs. Accountability is of key importance, and all employees should be responsible for all information they hold. Because social engineers use deception as their main tool, it is important to be observant when giving out information. Without exception, it is essential to authenticate the receiver of the information, since a social engineer often impersonates in order to deceive the victim.

Security is vital to continued business success. As such, we recommend using some combination of the following tools: videos, newsletters, brochures, signs, posters, screensavers, note pads, t-shirts, stickers, pictures of e-mail phishing, and audio clips. A problem with the tools that the employees see every day is that they become monotonous and eventually ignored. Therefore, educational material needs to appeal to all the senses and frequently be changed to be most useful. In addition to these awareness tools, an internal website dedicated to security information, including social-engineering information, is a good way to keep all personnel informed, educated and vigilant. Authentic stories of social-engineering attacks, safety tips and informational stories posted on the intranet or in e-mail are helpful for educating employees regarding social-engineering risks. Using authentic stories when educating employees increases their resistance to social-engineering exploits (Arthurs, 2002).

C. MULTIMODAL TRAINING

Another very efficient countermeasure to social engineering is multimodal training. The training that firefighters go through, in order to be competent when fire strikes, can save lives. Similarly, the training that employees within an organization receive can impede a social engineer from accessing secured computer networks and threaten national security, which can also save lives. If we agree that prevention and countering social-engineering attacks is essential for operational security, we must train with techniques analogous to those used to train firefighters.

Multimodal training is simulated training that incorporates scenario-based learning with live attacker-victim interactions. Scenario-based learning occurs in a context, situation, or social framework. It is based on the theory of situated cognition, which states that knowledge cannot be known and fully understood independent of its context (Kindley, 2002). Rather than simply making employees sit through boring one-way lectures, using interactive two-way simulations better conveys the dynamic nature of

social-engineering attacks. Live-action scenarios enable the participants to more realistically experience social-engineering attacks. The participant learns to react appropriately through recognition and practice.

Multimodal training is based on interactive scenarios which, in turn, are grounded in the underlying close-access techniques that are utilized by social engineers in the situations described above. Since it is not possible to create all possible social-engineering scenarios, it is sufficient to strive for scenarios that are as realistic as possible and that exemplify how the close-access techniques are carried out in different situations and for different target victims. The participant's level of preparedness concerning how to handle real-life attacks can be dramatically increased given sufficient practice. In order for this to work, however, the practice environment must be as similar as possible to the situations they are likely to encounter in the real world (Rotem, 2005).

This type of training requires the learner to take action instead of simply listening. These exercises utilize more of the five senses by emulating various attack situations. Using audio, visual, a simulated attacker and a simulated environment, the interactive training could present illicit requests and highlight the appropriate choices that employees should make when they are confronted by an actual social engineer. The goal is for this multimodal training to take people from a state of not knowing how to act in an information-dispatching situation to a state where they know how to successfully thwart social-engineering attacks.

D. FUTURE WORK

Since social engineering is a diverse and complex phenomenon, the prevention and countermodels to be used when fighting social engineering must contend with this complexity. The overall goal of the educational model described here is to increase awareness of how a social engineer performs an attack and how one can protect against such attacks. Knowledge of attacks is helpful in fighting them, so social-engineering attacks, both those that succeed and those that fail, should be made public whenever possible. Learning from mistakes and improving prevention must override any concerns regarding bad reputation or loss of business.

Long-term research should focus on educating future leaders and commanders concerning the social-engineering threat. Additionally, organizational policy must grant enough authority to question management in order to counter the attack of a social engineer impersonating management. With these defense-in-depth recommendations, the user should be able to recognize the different approaches of the social engineer and be able to act accordingly. Lastly, research into the methods of phishing is recommended. Phishing is one of the most prevalent and costly forms of social engineering today, and its growth represents an even greater threat for the future.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1] Abdul-Rahman, A. & Hailes, S. “A Distributed Trust Model”, ACM New Security Paradigms Workshop, 1997.

[2] Barber, R. “Social Engineering: A People Problem?” Network security, volume 2001, issue 7, July 2001.

[3] Chen, S., & Chaiken, S. The heuristic-systematic model in its broader context. In S. Chaiken & Y. Trope (Eds.), “Dual-process theories in social psychology” (pp. 73-96). New York: Guilford.

[4] Cialdini, R. B. “Influence: Science and Practice”, Allyn and Bacon. Needham Heights, MA; February 2001.

[5] Dalrymple, M. “Auditors Find IRS Employees Vulnerable To Hackers Posing As Information Technology Employees”. Security Focus. 16 March 2006. The Associated Press. 16 March 2006. http://www.securityfocus.com/news/10708.

[6] Gambetta, D. “Can We Trust Trust?” In, Trust: Making and Breaking Cooperative Relations, Gambetta, D (ed.). Basil Blackwell. Oxford, 1990, pp. 213-237.

[7] Granger, S. “Social Engineering Fundamentals, Part I: Hacker Tactics”, last updated 18 December 2001. Security Focus. 16 March 2006 <http://www.securityfocus.com/infocus/1527>.

[8] ---“Social Engineering Fundamentals, Part II: Combat Strategies”, 9 January 2002. Security Focus. 16 March 2006.

[9] Gulati, R. “The Threat of Social Engineering and Your Defense Against It”, SANS Reading Room. 2003. GIAC Security Essentials Certification Practical Assignment, 15 March 2006 <http://www.sans.org>.

[10] Hermansson, M. & Ravne, R. “Fighting Social Engineering”, University of Stockholm / Royal Institute of Technology, March 2005.

[11] Hung, Y., Dennis, A. & Robert, L. “Trust in Virtual Teams: Towards an Integrative Model of Trust Formation”, Proceedings of the 37th Hawaii International Conference on System Sciences – 2004.

[12] Kindley, R. W. “Scenario-Based E-Learning: A Step Beyond Traditional E-Learning” Learning Circuits-American Society for Training and Development, May 2002.

[13] Luhmann, N. “Risk: A Sociological Theory”, New York: Aldine de Gruyter; 1994.

[14] Mayer, R. C. and Davies, J. H. “An Integrative Model of Organizational Trust”, Academy of Management Review, Vol. 20 No. 3, 709-734; 1995.

[15] McDermott, J. “Social engineering – The Weakest Link in Information Security”. Window Security. 7 September 2005. Network Security Library :: Network Security. 16 March 2006. <http://www.secinf.net/Network_Security/Social-Engineering-The-Weakest-Link.html>

[16] Mitnick, K. D. and Simon, W. L. “The Art of Deception”, Wiley Publishing, Inc. Indianapolis, Indiana; 2002.Petty, R. E., & Wegener, D. T. The elaboration likelihood model: Current status and controversies. In S. Chaiken & Y. Trope (Eds.), Dual-process theories in social psychology (pp. 41-72). New York: Guilford.

[17] Rowe, N. C. “A Taxonomy of Deception in Cyberspace”, International Conference in Information Warfare and Security, Princess Anne, MD, March 2006.

[18] Rotem, A. et al, “Guidelines for development of scenario based e-learning resources” www.anaphi.unsw.edu.au/Scenario_guidelines.pdf, January 2005.

[19] “Social Engineering (computer security)”. Wikipedia. 15 March 2006 http://en.wikipedia.org/wiki/Social_engineering_(computer_security)

[20] “System Administration”, SANS Information Security Reading Room, 15 March 2006. <http://www.sans.org>.

[21] Sztompka, P. “Trust”, Cambridge University Press. New York, NY; 1999.

BIBLIOGRAPHY

[1] Granger, S. "Social Engineering Fundamentals, Part I: Hacker Tactics", last updated 18 December 2001. Security Focus. 16 March 2006 <http://www.securityfocus.com/infocus/1527>.

A. Ameritech Consumer Information "Social Engineering Fraud," http://www.ameritech.com/content/0,3086,92,00.html

B. Anonymous "Social engineering: examples and countermeasures from the real-world," Computer Security Institute, http://www.gocsi.com/soceng.htm.

C. Arthurs, W. "A Proactive Defence to Social Engineering," SANS Institute, August 2, 2001. http://www.sans.org/infosecFAQ/social/defence.htm

D. Berg, Al: "Al Berg Cracking a Social Engineer," by, LAN Times November. 6, 1995. http://packetstorm.decepticons.org/docs/social-engineering/soc_eng2.html

E. Bernz 1: "Bernz's Social Engineering Intro Page", http://packetstorm.decepticons.org/docs/social-engineering/socintro.html

F. Bernz 2: "The Complete Social Engineering FAQ!" http://packetstorm.decepticons.org/docs/social-engineering/socialen.txt

G. Harl "People Hacking: The Psychology of Social Engineering" Text of Harl's Talk at Access All Areas III, March 7, 1997. http://packetstorm.decepticons.org/docs/social-engineering/aaatalk.html

H. Mitnick, K. "My First RSA Conference," Security Focus, April 30, 2001 http://www.securityfocus.com/news/199.

I. Orr, C. "Social Engineering: A Backdoor to the Vault,", SANS Institute, September 5, 2000. http://www.sans.org/infosecFAQ/social/backdoor.htm

J. Palumbo, J. "Social Engineering: What is it, why is so little said about it and what can be done?", SANS Institute, July 26, 2000, http://www.sans.org/infosecFAQ/social/social.htm

K. Stevens, G. "Enhancing Defenses Against Social Engineering" SANS

Institute, March 26, 2001,
http://www.sans.org/infosecFAQ/social/defense_social.htm.
L. Tims, R. “Social Engineering: Policies and Education a Must” SANS Institute, February 16, 2001, http://www.sans.org/infosecFAQ/social/policies.htm.
M. Verizon “PBX Social Engineering Scam” 2000,
http://www.bellatlantic.com/security/fraud/pbx_scam.htm.
N. VIGILANTe “Social Engineering” 2001,
http://www.vigilante.com/inetsecurity/socialengineering.htm.

[2] ---“Social Engineering Fundamentals, Part II: Combat Strategies”, 9 January. 2002. Security Focus. 16 March 2006.

A. Arthurs, W. “A Proactive Defence to Social Engineering,” SANS Institute, August 2, 2001. http://www.sans.org/infosecFAQ/social/defence.htm
B. Berg, A. “Cracking a Social Engineer,” LAN Times, November. 6, 1995. http://packetstorm.decepticons.org/docs/social-engineering/soc_eng2.html
C. Fine, N. “A World-Class Confidential Information and Intellectual Property Protection Strategy”, Pro-Tec Data, 1998. http://www.pro-tecdata.com/articles/world-class.html
D. Harl: “People Hacking: The Psychology of Social Engineering” Text of Harl’s Talk at Access All Areas III, March 7, 1997.
http://packetstorm.decepticons.org/docs/social-engineering/aaatalk.html
E. Nelson, R. “Methods of Hacking: Social Engineering,” the Institute for Systems Research, University of Maryland, 2001.
http://www.isr.umd.edu/gemstone/infosec/ver2/papers/socialeng.html
F. Stevens, G. “Enhancing Defenses Against Social Engineering” SANS Institute, March 26, 2001,
http://www.sans.org/infosecFAQ/social/defense_social.htm.
G. Verizon “PBX Social Engineering Scam” 2000,
http://www.bellatlantic.com/security/fraud/pbx_scam.htm.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. OSD
   Directorate of Operational Testing and Evaluation
   ATTN: Mr. Stephen Gates
   Washington, DC

4. MICHAEL A. SHEPHERD, Col, USAFR
   318 IOG/CD-AO
   San Antonio, Texas

5. VINCENT D. CRABB, Lt Col, USA
   Joint OPSEC Support Center
   San Antonio, Texas